

WHAT IS CLAIMED IS:

1. A method comprising:
 - receiving, by a service provider computer, a transaction initiation message from a token requestor computer;
 - transmitting, by the service provider computer to a token service computer, a request message comprising a token requestor identifier associated with the token requestor, and a service provider computer identifier associated with the service provider computer;
 - responsive to transmitting the cryptogram request message, receiving, by the service provider computer, a response message comprising a token and/or a cryptogram;
 - generating, by the service provider computer, an authorization request message comprising the token and the cryptogram;
 - transmitting, by the service provider computer, the authorization request message to a processing computer in communication with a token service computer, wherein the processing computer, in conjunction with the token service computer, determines a real credential associated with the token and validates the cryptogram; and
 - responsive to transmitting the authorization request message, receiving, by the service provider computer, an authorization response message from the processing computer.
2. The method of claim 1, wherein the cryptogram is a channel-specific cryptogram that is only valid in a particular interaction channel.
3. The method of claim 1, wherein the request message is a cryptogram request message further comprising the token or a token identifier, and wherein the token service computer validates that the token, the token requestor identifier associated with the token requestor, and the service provider computer identifier are associated with each other before generating the cryptogram.
4. The method of claim 3, wherein the token service computer comprises a table mapping the service provider identifier with the token requestor identifier.

5. The method of claim 3, wherein transmitting, by the service provider computer to the token service computer, the cryptogram request message comprising the token or token identifier, the token requestor identifier associated with the token requestor, and the service provider computer identifier associated with the service provider computer comprises transmitting, by the service provider computer to the token service computer, the cryptogram request message comprising the token identifier, the token requestor identifier associated with the token requestor, and the service provider computer identifier associated with the service provider computer.

6. The method of claim 1, wherein the token requestor is a resource provider computer.

7. The method of claim 1, wherein the token is mathematically generated from the real credential.

8. The method of claim 1, wherein the token requestor computer received an interaction request from a user device associated with a user.

9. The method of claim 1, wherein the request message is encrypted with a cryptographic key of a first cryptographic key pair that is shared between the token service computer and the service provider computer, wherein the first cryptographic key pair is different than a second cryptographic key pair shared between the token requestor computer and the service provider computer.

10. A service provider computer comprising:
a processor; and
a non-transitory computer readable medium, comprising instructions, that when executed by the processor, cause the processor to
receive a transaction initiation message from a token requestor computer;
transmit, to a token service computer, a request message comprising a token requestor identifier associated with the token requestor, and a service provider computer identifier associated with the service provider computer;

responsive to transmitting the cryptogram request message, receive a response message comprising a token and/or a cryptogram;

generate an authorization request message comprising the token and the cryptogram;

transmit the authorization request message to a processing computer in communication with a token service computer, wherein the processing computer, in conjunction with the token service computer, determines a real credential associated with the token and validates the cryptogram; and

responsive to transmitting the authorization request message, receive an authorization response message from the processing computer.

11. The service provider computer of claim 10, wherein the request message is a cryptogram request message and comprises the token.

12. The service provider computer of claim 10, wherein the token requestor identifier is a token requestor ID and the service provider computer identifier is a token requestor-token service provider ID.

13. The service provider computer of claim 10, wherein the cryptogram is formed from the token requestor identifier and the service provider computer identifier.

14. The service provider computer of claim 10, wherein the real credential is a PAN.

15. A method comprising:
transmitting, by a service provider computer to a token service computer, a token request message comprising a service provider identifier associated with the service provider computer, and a token requestor identifier associated with a token requestor of a plurality of token requestors operatively coupled to the service provider system;
in response to transmitting the token request message, receiving, by the service provider computer from the token provider system, a token; and
transmitting, by the service provider computer to the token requestor, the token.

16. The method of claim 15, wherein the token provider system comprises a database comprising a table mapping the service provider identifier with the token requestor identifier.

17. The method of claim 15, wherein the token request message or data contained in the token request message is encrypted using a cryptographic key of a first cryptographic key pair used to secure communications between the service provider computer and the token service computer.

18. The method of claim 17, wherein the service provider system and the token requestor use a second cryptographic key pair to secure communications between the service provider system and the token requestor, the token being encrypted with a cryptographic key of the second cryptographic key pair when it is transmitted from the service provider computer to the token requestor.

19. The method of claim 15, wherein the token is 16 digits long.

20. The method of claim 15, wherein the token request message or data contained in the token request message is encrypted using a cryptographic key of a first cryptographic key pair used to secure communications between the service provider computer and the token service computer, and wherein the service provider system and the token requestor use a second cryptographic key pair to secure communications between the service provider system and the token requestor, the token being encrypted with a cryptographic key of the second cryptographic key pair when it is transmitted from the service provider computer to the token requestor, and wherein the first cryptographic key pair and the second cryptographic key pair are each symmetric key pairs.